CLAIMS

1. A network based anti-virus system especially for wide area networks, like the Internet, comprising:

client computer(s), which are any computers in the network;

anti-virus host computer(s), which are any computers in the network chosen for that purpose;

wherein identification(s) of file(s) or other web content is delivered from a client computer to an anti-virus host computer;

wherein said anti-virus host computer compares each of said delivered identification(s) to stored identifications of files or other web content, and on the basis of the results of said comparison either:

(a) it is performed safety measures,

(b) and / or, said client computer and / or the user of said client computer is informed about the results of said comparison,

(c) or, no specific actions are performed.

2. A network based anti-virus system according to claim 1, comprising:

wherein a said stored identification either:

(a) belongs to a specific file or other web content,

(b) does not belong to any specific file or other web content, but is rather an identification filter,

(c) or, partly belongs to a specific file or other web content, and partly is a said identification filter.

3. A network based anti-virus system according to claim 2, comprising:

wherein said delivered identification(s) is delivered when said client computer downloads from the network said file(s) or other web content to which said delivered identification(s) belong.

4. A network based anti-virus system according to claim 3, comprising:

wherein said delivered identification(s) is delivered to said anti-virus host computer either:

(a) before said downloading,

(b) during said downloading,

(c) or, after said downloading.

5. A network based anti-virus system according to claim 4, comprising:

wherein said stored identifications of files are stored identifications of known virus infected files;

wherein said stored identifications of other web content are stored identifications of other known virus infected web content;

wherein said stored identifications are in a database kept by said anti-virus host computer;

wherein said (a) and / or (b) type actions which are performed on the basis of the results of said comparison, are performed when a said delivered identification matches or resembles in certain extent any of said stored identifications;

wherein said safety measures are performed by requesting / causing said client computer and optionally also said anti-virus host computer to perform safety measures.

6. A network based anti-virus system according to claim 5, comprising:

wherein a said delivered identification consists of:

(a) file identification information,

(b) and / or, data identification information;

wherein a said stored identification consists of:

(a) file identification information,

(b) and / or, data identification information;

wherein said file identification information comprises one or more of the following properties of the file or other web content to which said file identification belongs:

(a) source URL-address or other type of address,

(b) source computer URL-address or other type of address,

(c) name,

(d) type,

(e) content type,

(f) size,

(g) creation date,

(h) version number,

(i) publisher,

(j) authentication certificate,

(k) or, other properties;

wherein said data identification information of the file or other web content to which said data identification belongs, comprises:

(a) a check-sum or any identification value based upon the data of said file or other web content,

(b) and / or, data sample picked according to a certain pattern, algorithm or other rule from said file or other web content,

(c) or, all data of said file or other web content;

wherein said file identification information and said data identification information is delivered to said anti-virus host computer either:

(a) solely from said client computer,

(b) solely from the respective source host computer(s) of said file(s) or other web content which file identification information and data identification information it is question of,

(c) or, partly from said client computer and partly from said respective source host computer(s).

7. A network based anti-virus system according to claim 5, comprising:

wherein said requesting / causing to perform said safety measures is done by said anti-virus host computer;

wherein said informing about the results of said comparison is done by said anti-virus host computer;

wherein said safety measures comprise one or more of the following:

(a) said client computer performs a virus scan for said file(s) or other web content which said anti-virus host computer has determined to be a security threat in certain extent,

(b) said client computer sends said security threat file(s) or other web content to be virus scanned by said anti-virus host computer,

(c) said client computer destroys said security threat file(s) or other web content,

(d) said client computer performs a virus scan in said client computer, the software for said virus scan optionally being provided by said anti-virus host computer;

wherein optionally said anti-virus host computer alternatively acquires independently said security threat file(s) or other web content, and performs a virus scan for said security threat file(s) or other web content.

8. A network based anti-virus system according to claim 5, comprising:

wherein said anti-virus host computer optionally informs / alarms said client computer and / or the user of said client computer only if the results of said comparison indicate a security threat or potential security threat, and optionally provides for said client computer and / or the user of said client computer a risk rating depicting the level of said security threat;

wherein said anti-virus host computer optionally informs said client computer and / or the user of said client computer about the results of said comparison regardless of the type of said results, and optionally provides for said client computer and / or the user of said client computer a risk rating depicting the level of security threat indicated by said results.

9. A network based anti-virus system according to claim 5, comprising:

wherein said anti-virus host computer keeps database of the identifications of the files and / or other web content which the client computers or the users of client computers have downloaded from the network, each said identification being stored in said database in connection of the respective downloading of said file or other web content to which said identification belongs;

wherein said anti-virus host computer retains information about one or more of the following:

(a) old and / or newly detected virus infections,

(b) old and / or newly detected security threats,

(c) old and / or newly determined security risk ratings,

(d) personal download statistics,

for the files and / or other web content which a client computer or the user of said client computer has earlier downloaded from the network, said client computer and / or the user of said client computer being optionally able to access said anti-virus host computer retained information;

wherein said anti-virus host computer informs / alerts the respective client computer and / or the user of said respective client computer, when said anti-virus host computer retained information on the part of any of (a) through (c) changes in certain way;

wherein if said anti-virus host computer announces said anti-virus host computer retained information on the part of any of (a) through (c) to have changed alarming enough for certain files(s) or other web content, then the respective client computer optionally:

(a) destroys said file(s) or other web content from said client computer,

(b) and / or, performs a virus scan in said client computer, the software for said virus scan optionally provided by said anti-virus host computer.

10. A network based anti-virus system according to claim 4, comprising:

wherein said anti-virus host computer does not specifically fight against viruses;

wherein the purpose of said comparison is to find out if said inspected files and other web content are or are not non-wanted / unacceptable instead of if they are possibly virus infected.

11. A network based anti-virus system according to claim 10, comprising:

wherein said stored identifications of files are stored identifications of known non-wanted / unacceptable files;

wherein said stored identifications of other web content are stored identifications of other known non-wanted / unacceptable web content.

12. A network based anti-virus system according to claim 5, comprising:

wherein said other web content comprises one or more of the following:

(a) web pages,
(b) independent program scripts or other client computer processed components,
(c) e-mail messages,
(d) e-mail message attachments,
(e) or, any data which a client computer can download from the network.

13. A network based anti-virus system according to claim 1, comprising:

wherein it is not done said identification comparison, and said identification(s) of said file(s) or other web content is not delivered to an anti-virus host computer;

wherein an anti-virus host computer provides to a client computer a list of one or more of the following harmful or potentially harmful:

(a) files or other web content,
(b) publishers,
(c) web sites,
(d) host computers;

wherein when said client computer downloads file(s) or other web content from the network, said client computer compares identification(s) of said file(s) or other web content to the items in said client computer retained list, and if a said identification matches in certain extent any of said items, then:

(a) it is performed safety measures,

(b) and / or, said client computer notifies the user of said client computer about the results of said client computer performed comparison.

14. A network based anti-virus system according to claim 3, comprising:

intermediate computer(s), which are able to prevent downloading of files and / or other web content from the network to a client computer.

15. A network based anti-virus system according to claim 14, comprising:

wherein a said intermediate computer is:

(a) a server of the local area network,

(b) a server of the internet service provider,

(c) a network node computer,

(d) or, a source host computer from which a client computer downloads file(s) or other web content.

16. A network based anti-virus system according to claim 14, comprising:

wherein said stored identifications of files are stored identifications of known virus infected files;

wherein said stored identifications of other web content are stored identifications of other known virus infected web content;

wherein said stored identifications are in a database kept by said anti-virus host computer;

wherein said (a) and / or (b) type actions which are performed on the basis of the results of said comparison, are performed when a said delivered identification matches or resembles in certain extent any of said stored identifications;

wherein said safety measures are performed by requesting / causing one or more of the following computers to perform safety measures:

(a) a said intermediate computer,

(b) said client computer,

(c) said anti-virus host computer.

17. A network based anti-virus system according to claim 16, comprising:

wherein a said delivered identification consists of:

(a) file identification information,

(b) and / or, data identification information;

wherein a said stored identification consists of:

(a) file identification information,

(b) and / or, data identification information;

wherein said file identification information comprises one or more of the following properties of the file or other web content to which said file identification belongs:

(a) source URL-address or other type of address,

(b) source computer URL-address or other type of address,

(c) name,

(d) type,

(e) content type,

(f) size,

(g) creation date,

(h) version number,

(i) publisher,

(j) authentication certificate,

(k) or, other properties;

wherein said data identification information of the file or other web content to which said data identification belongs, comprises:

(a) a check-sum or any identification value based upon the data of said file or other web content,

(b) and / or, data sample picked according to a certain pattern, algorithm or other rule from said file or other web content,

(c) or, all data of said file or other web content;

wherein said file identification information and said data identification information is delivered to said anti-virus host computer either:

(a) solely from a said intermediate computer,

(b) solely from the respective source host computer(s) of said file(s) or other web content which file identification information and data identification information it is question of,

(c) or, partly from a said intermediate computer and partly from said respective source host computer(s).

18. A network based anti-virus system according to claim 16, comprising:

wherein said requesting / causing to perform said safety measures is done by said anti-virus host computer;

wherein said informing about the results of said comparison is done by a said intermediate computer;

wherein said safety measures comprise one or more of the following:

(a) a said intermediate computer performs a virus scan for said file(s) or other web content which said anti-virus host computer has determined to be a security threat in certain extent,

(b) a said intermediate computer sends said security threat file(s) or other web content to be virus scanned by said anti-virus host computer,

(c) a said intermediate computer prevents the download of said security threat file(s) or other web content through said intermediate computer;

wherein optionally said anti-virus host computer alternatively acquires independently said security threat file(s) or other web content, and performs a virus scan for said security threat file(s) or other web content.

19. A network based anti-virus system according to claim 18, comprising:

wherein a said intermediate computer optionally informs / alarms said client computer and / or the user of said client computer only if the results of said comparison indicate a security threat or potential security threat, and optionally provides for said client computer and / or the user of said client computer a risk rating given by said anti-virus host computer, said risk rating depicting the level of said security threat;

wherein a said intermediate computer optionally informs said client computer and / or the user of said client computer about the results of said comparison regardless of the type of said results, and optionally provides for said client computer and / or the user of said client computer a risk rating given by said anti-virus host computer, said risk rating depicting the level of security threat indicated by said results.

20. A network based anti-virus system according to claim 14, comprising:

wherein said anti-virus host computer does not specifically fight against viruses;

wherein the purpose of said comparison is to find out if said inspected files and other web content are or are not non-wanted / unacceptable instead of if they are possibly virus infected.

21. A network based anti-virus system according to claim 20, comprising:

wherein said stored identifications of files are stored identifications of known non-wanted / unacceptable files;

wherein said stored identifications of other web content are stored identifications of other known non-wanted / unacceptable web content.

22. A network based anti-virus system according to claim 16, comprising:

wherein said other web content comprises one or more of the following:

(a) web pages,

(b) independent program scripts or other client computer processed components,

(c) e-mail messages,

(d) e-mail message attachments,

(e) or, any data which a client computer can download from the network.

23. A network based anti-virus system according to claim 14, comprising:

wherein it is not done said identification comparison, and said identification(s) of said file(s) or other web content is not delivered to an anti-virus host computer;

wherein an anti-virus host computer provides to a said intermediate computer a list of one or more of the following harmful or potentially harmful:

(a) files or other web content,

(b) publishers,

(c) web sites,

(d) host computers;

wherein when a client computer downloads file(s) or other web content from the network, said intermediate computer compares identification(s) of said file(s) or other web content to the items in said intermediate computer retained list, and if a said identification matches in certain extent any of said items, then:

(a) it is performed safety measures,

(b) and / or, said intermediate computer notifies said client computer and / or the user of said client computer about the results of said intermediate computer performed comparison.

24. A network based anti-virus system especially for wide area networks, like the Internet, comprising:

a client computer, which is any computer in the network;

an intermediate computer which is able to prevent downloading of files and / or other web content from the network to said client computer;

wherein when said client computer downloads a file or other web content from the network, and if the identification of said file or other web content matches or resembles in certain extent any of the identifications in a database of the identifications of known virus infected files or other virus infected web content, then said intermediate computer:

(a) prevents said download of said file or other web content,

(b) or, requests / causes said client computer to destroy said file or other web content from said client computer if said client computer has already downloaded said file or other web content,

(c) and / or, optionally informs said client computer or the user of said client computer about said security threat;

wherein said identifications in said database are not signatures of virus code, but rather represent the identities of the virus infected files or other virus infected web content self;

wherein a said identification in said database either:

(a) belongs to a specific file or other web content,

(b) does not belong to any specific file or other web content, but is rather an identification filter,

(c) or, partly belongs to a specific file or other web content, and partly is a said identification filter.

25. A network based anti-virus system according to claim 24, comprising:

wherein said intermediate computer is:

(a) a server of the local area network,

(b) a server of the internet service provider,

(c) a network node computer,

(d) or, a source host computer from which said client computer downloads file(s) or other web content.

26. A network based anti-virus system according to claim 24, comprising:

wherein a said identification in said database consists of:

(a) file identification information,

(b) and / or, data identification information;

wherein said identification of said inspected file or other web content consists of:

(a) file identification information,

(b) and / or, data identification information;

wherein said file identification information comprises one or more of the following properties of the file or other web content to which said file identification belongs:

(a) source URL-address or other type of address,

(b) source computer URL-address or other type of address,

(c) name,

(d) type,

(e) content type,

(f) size,

(g) creation date,

(h) version number,

(i) publisher,

(j) authentication certificate,

(k) or, other properties;

wherein said data identification information of the file or other web content to which said data identification belongs, comprises:

(a) a check-sum or any identification value based upon the data of said file or other web content,

(b) and / or, data sample picked according to a certain pattern, algorithm or other rule from said file or other web content,

(c) or, all data of said file or other web content.

27. A network based download information system especially for wide area networks, like the Internet, comprising:

client computer(s);

a host computer which keeps database of the identifications of the files and / or other web content which the client computers or the users of client computers have downloaded from the network, each said identification being stored in said database in connection of the respective downloading of said file or other web content to which said identification belongs;

wherein said host computer retains information about one or more of the following:

(e) old and / or newly detected virus infections,

(f) old and / or newly detected security threats,

(g) old and / or newly determined security risk ratings,

(h) personal download statistics,

for the files and / or other web content which a client computer or the user of said client computer has earlier downloaded from the network, said client computer and / or the user of said client computer being optionally able to access said host computer retained information;

wherein said host computer informs / alerts the respective client computer and / or the user of said respective client computer, when said host computer retained information on the part of any of (a) through (c) changes in certain way;

wherein if said host computer announces said host computer retained information on the part of any of (a) through (c) to have changed alarming enough for certain files(s) or other web content, then the respective client computer optionally:

(c) destroys said file(s) or other web content from said client computer,

(d) and / or, performs a virus scan in said client computer, the software for said virus scan optionally provided by said host computer.